Рано выбрасывать iframe в 2022-м году

Андрей Кузнецов



Пару слов обо мне



- Верстка с 2005 года
- Флешер до 2012 года 
- Frontend Lead в компании «Рунет Бизнес Системы»

service.com

SHOP.com

Total 5$

Apple Pay Session

Pay

RENDER

click

<script src="https://service.com/lib.js">

redirect

API

service.com/child.html

lib-child.js

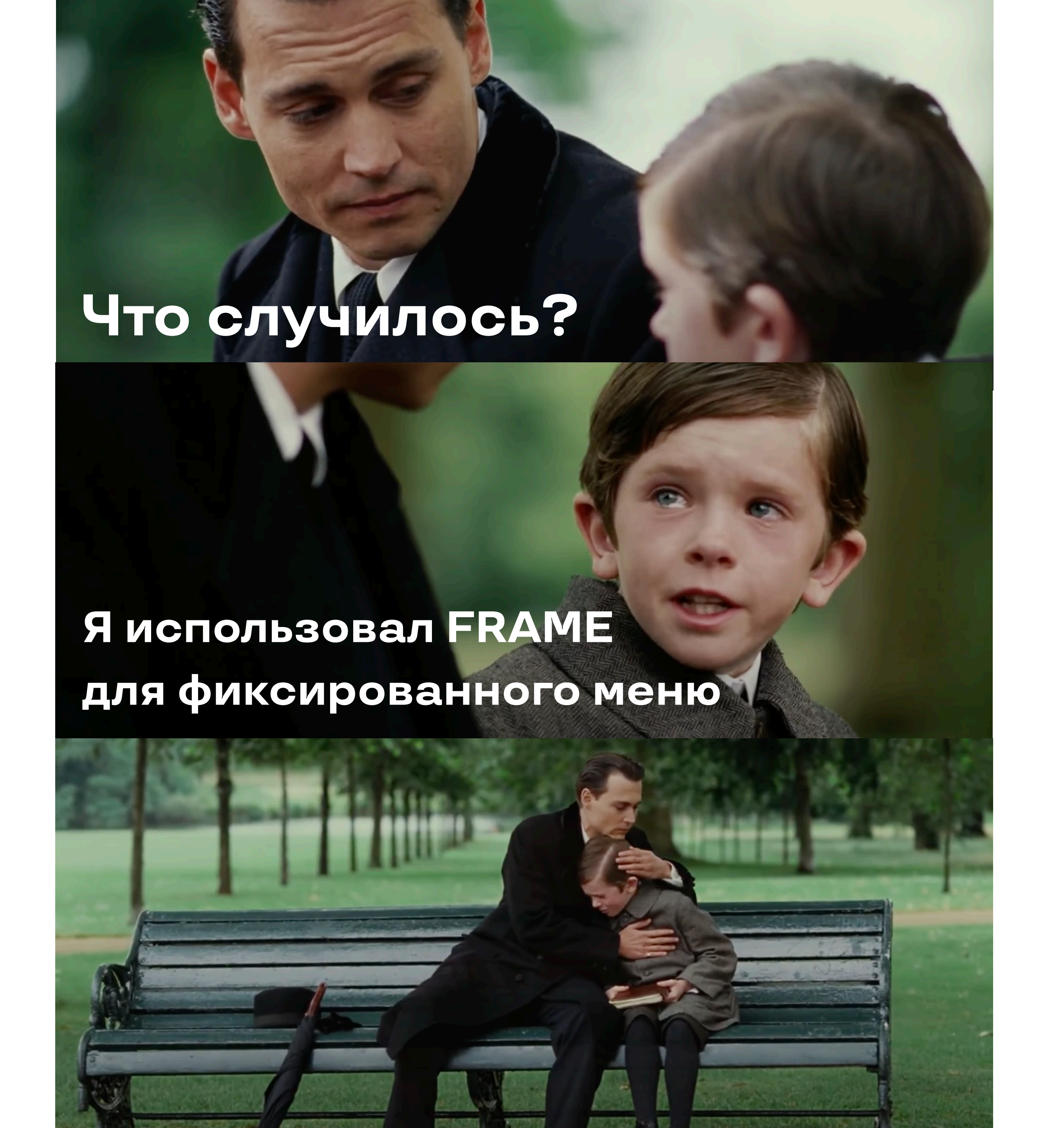


История ~~iframe~~ frame



История iframe




Что случилось?
Я использовал FRAME
для фиксированного меню



- Сведения о музее
- Совет школьного музея как Детская общественная организация
- Сергей Дмитриевич Василисин
- Поисковые проекты музея
- Исправляем ошибки
- Вторая жизнь героя
- Однополчане герои
- Над сайтом работали



Поисковые проекты музея



«Сила памяти, эмоциональная сила живых рассказов такова, что для них как бы не существует дистанции времени: будто с тобой это происходит... или у тебя на глазах» (А.Адамович о книгах С.Алексеевича).

Рассказ № | 1 | | 2 | | 3 | | 4 | | 5 | | 6 |



Рассказ №1

Мой известный неизвестный герой,



Война на совесть постаралась
Она Огонь и смерть на нас обрушив,
вошла не только в души,
Не только в памяти осталось...

Первый дар, который получает человек, появившийся на свет, имя. Каждое имя таит в себе особое значение. Не случайно ведь говорят: " По имени и житие ".
Именно дела, доброе имя остаётся после смерти человека, сохраняя память о нём. Война лишила многих героев имён, и так важно, чтобы память о них жила.

Никто не знает их фамилий,
О них ни песен нет, ни книг,
Здесь чей-то сын, и чей-то милый,
И чей-то первый ученик.
(Г. Казакова)



60 лет после войны. Жизнь целого поколения. Но до сих пор есть могилы неизвестного солдата, безымянные герои, а сколько без вести пропавших?

Открыто все своё писали имя,
Чтоб знали люди будущих времён,
Что подвиг сей свершенный всеми ими,
Во имя человечества свершён.

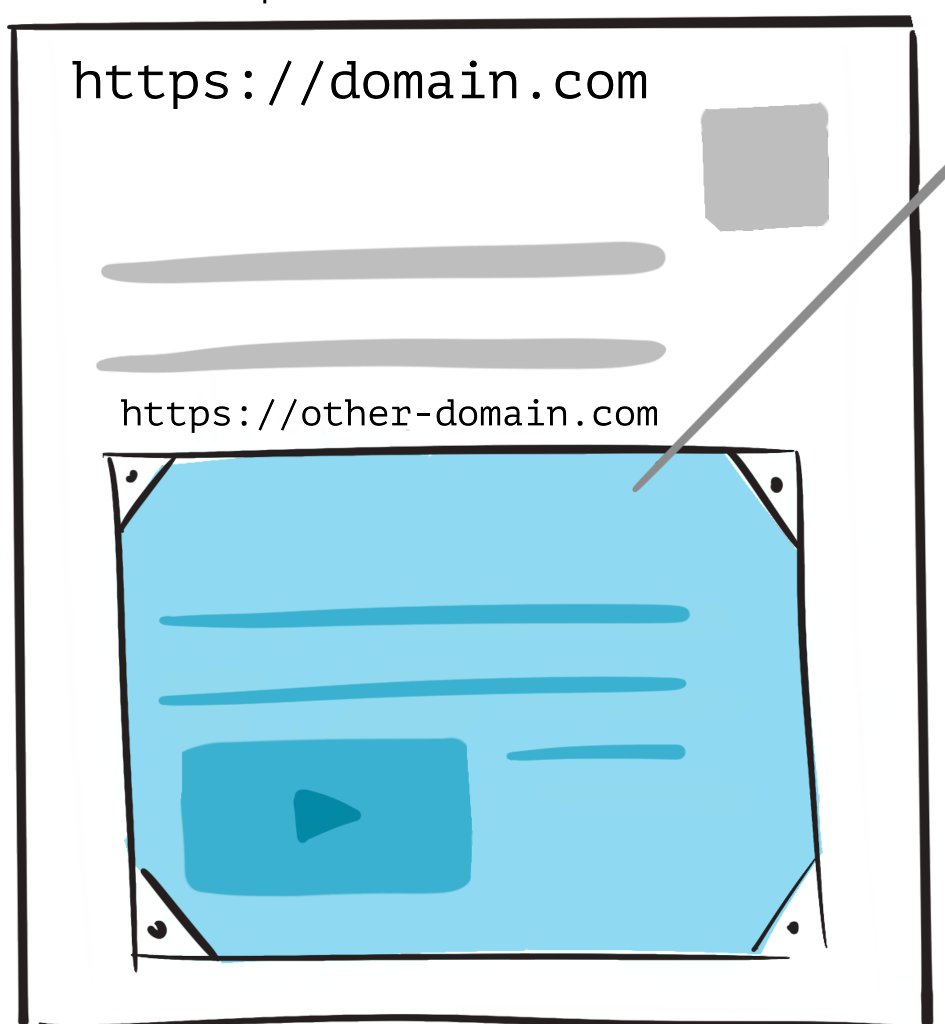
К чести нашей литературы, многих героев мы давно знаем по



История iframe



Кратко об iframe




```html
<iframe src="https://other-domain.com"/>
```

Кратко об iframe

- Загружает в область заданных размеров любые другие независимые документы
- Был слабо защищен, поэтому имеет плохую репутацию



Итого на 2022-й

- Полностью изолирован от родительского документа
- Не показывает изменение урла для родителя (если разные домены)
- Но он всё так же может ~~сломать страницу~~ мешать пользователю

iFrame

You shall not pass!



Sandbox

```
<iframe src="..." sandbox="значение"/>
```

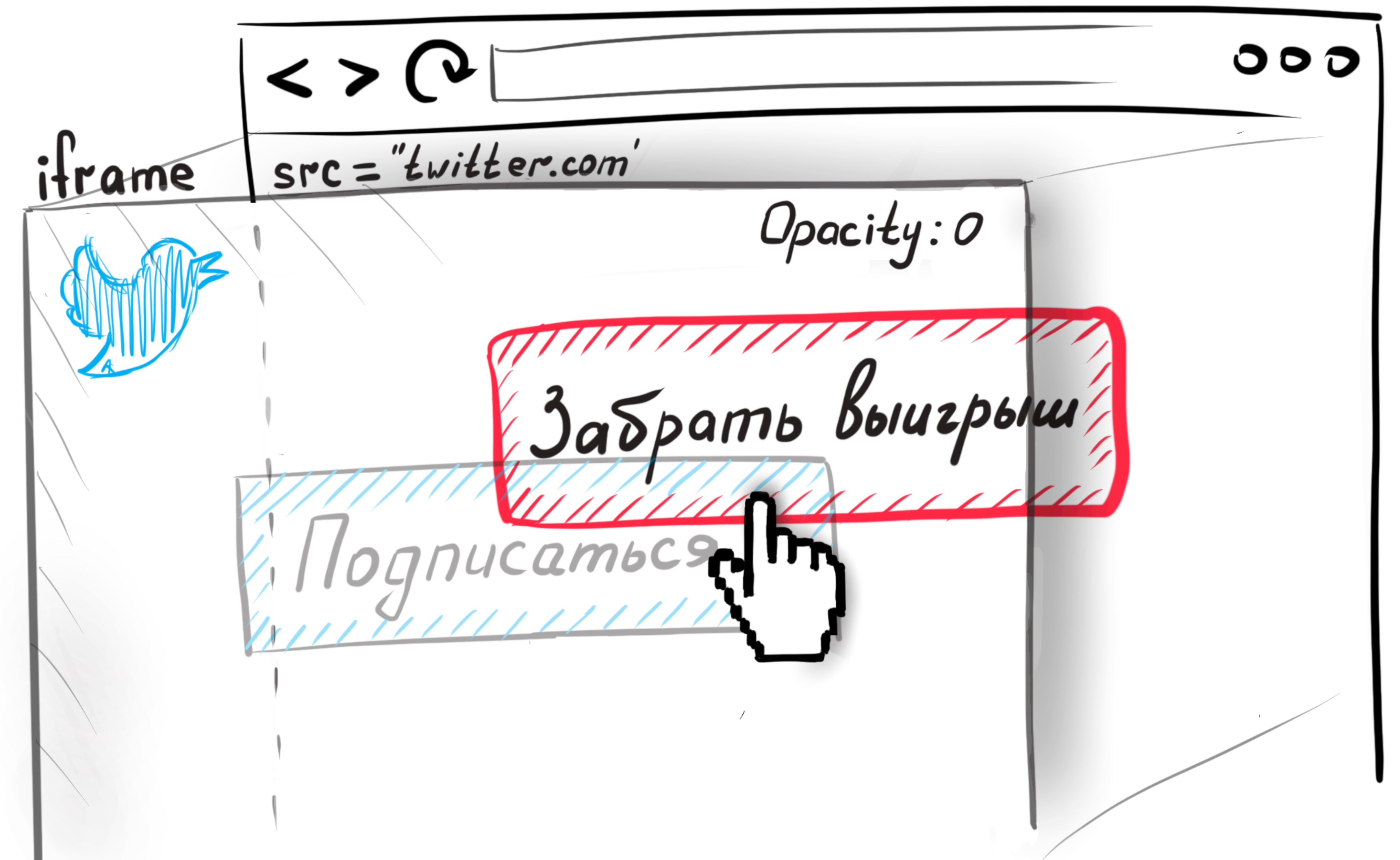
Пустое значение	Включить все ограничения
allow-forms	Разрешить отправку данных форм
allow-pointer-lock	Разрешить использование Pointer Lock API (захват движения мышью)
allow-popups	Разрешить всплывающие окна (window.open(), target="_blank" и др.)

. . .

Атака типа clickjacking



Clickjacking



Защита. Заголовок X-Frame-Options

DENY

- Никогда не показывать страницу внутри фрейма.

SAMEORIGIN

- Разрешить открытие страницы внутри фрейма только в том случае, если родительский документ имеет тот же источник.

ALLOW-FROM domain

- Разрешить открытие страницы внутри фрейма только в том случае, если родительский документ находится на указанном в заголовке домене.





Сайт **site.com** не позволяет установить соединение.

Защита. Заголовок X-Frame-Options

DENY

- Никогда не показывать страницу внутри фрейма.

SAMEORIGIN

- Разрешить открытие страницы внутри фрейма только в том случае, если родительский документ имеет тот же источник.

ALLOW-FROM domain

- Разрешить открытие страницы внутри фрейма только в том случае, если родительский документ находится на указанном в заголовке домене.



Защита. Content-Security-Policy

`frame-ancestors`

```
Content-Security-Policy: frame-ancestors 'self'
example.com *.example.net;
```

Защита. Закроемся div

```
<style>
  #protector {
    height: 100%; width: 100%; position: absolute;
    left: 0; top: 0; z-index: 99999999;
  }
</style>

<div id="protector">
  <a href="/" target="_blank">Перейти к сайту</a>
</div>

<script>
  if (top.document.domain == document.domain) {
    protector.remove();
  }
</script>
```

BITB (Browser In The Browser) attack

Делает фишинг практически незаметным

Log into Facebook | Facebook - Google Chrome

facebook.com/login.php?skip_api_login=1&api_key=525265914

ount

Phishing

Log Into Facebook

Email or phone number

Password

Log In

Forgot account?

or

Create new account

Not now

Log into Facebook | Facebook - Google Chrome

facebook.com/login.php?skip_api_login=1&api_key=525...

ook Create new account

Real

Log Into Facebook

Email or phone number

Password

Log In

Forgot account?

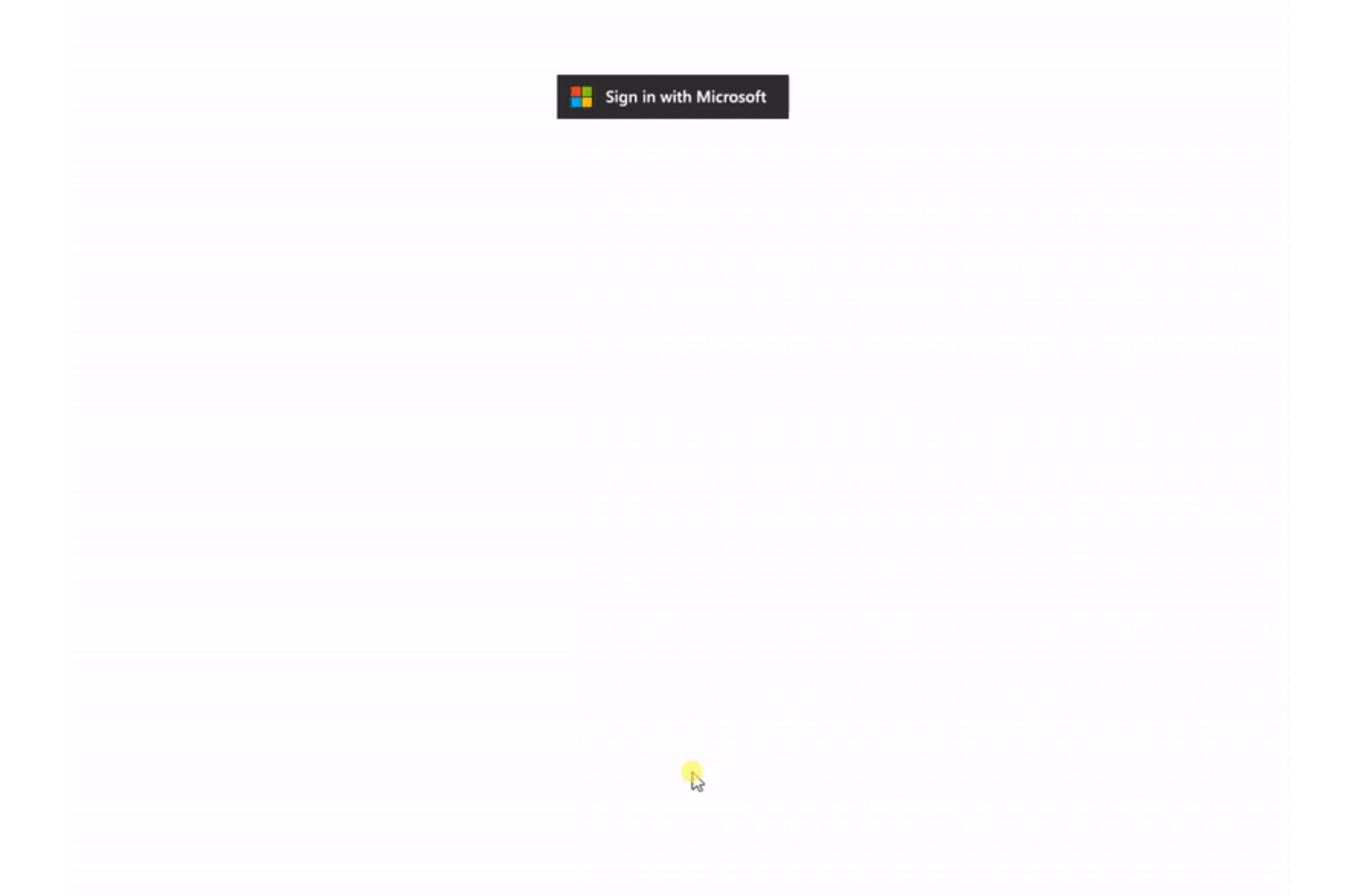
or

Create new account

Not now

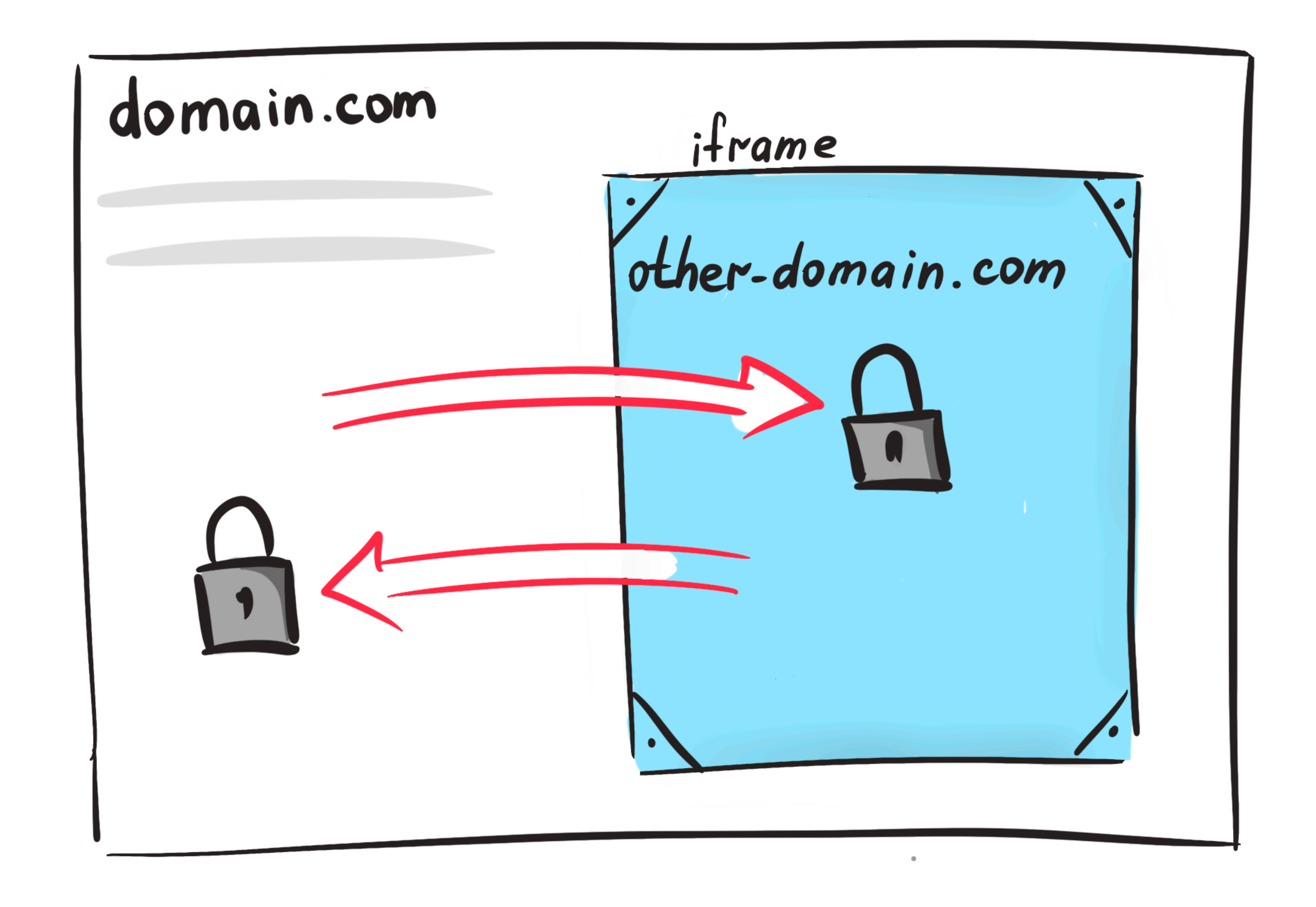


BITB (Browser In The Browser) attack



Можно ли получить доступ к iframe?

При условии, что разные домены



Можно, если договориться

PostMessage и "message"

```
otherWindow.postMessage(message, targetOrigin);
```

otherWindow

Ссылка на другое окно. Для iframe это parent.

message

Данные, которые нужно отправить в другое окно.

targetOrigin

Определяет источник для окна-получателя, только окно с данного источника имеет право получить сообщение.

Если мы не хотим проверять, то в targetOrigin можно указать *.



Пример. Закинем информацию в iframe

```
<iframe src="http://example.com" name="example">

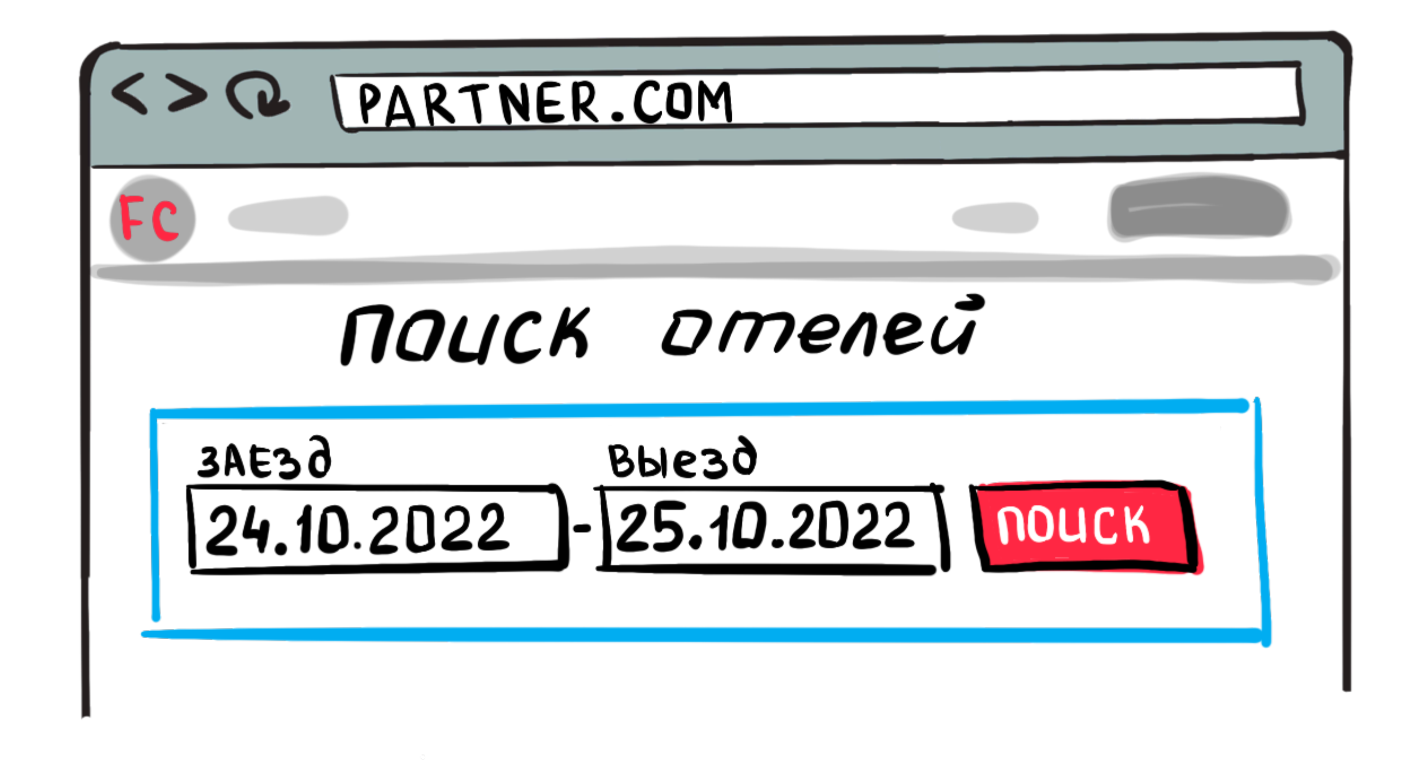
<script>
  let win = window.frames.example;
  win.postMessage("message", "http://example.com");
</script>
```

Пример. Ловим информацию в iframe

```
window.addEventListener("message", function(event) {
  if (event.origin != "http://frontendconf.ru") {
    // что-то пришло с неизвестного домена. Проигнорируем это
    return;
  }
  alert( "received:" + event.data );
  // Можно отправить ответ через event.source.postMessage(...)
});
```

Сила iframe 🤘

- Вам требуется создать виджет для встраивания на другие сайты?
- Это может быть от прогноза погоды до покупки авиабилетов

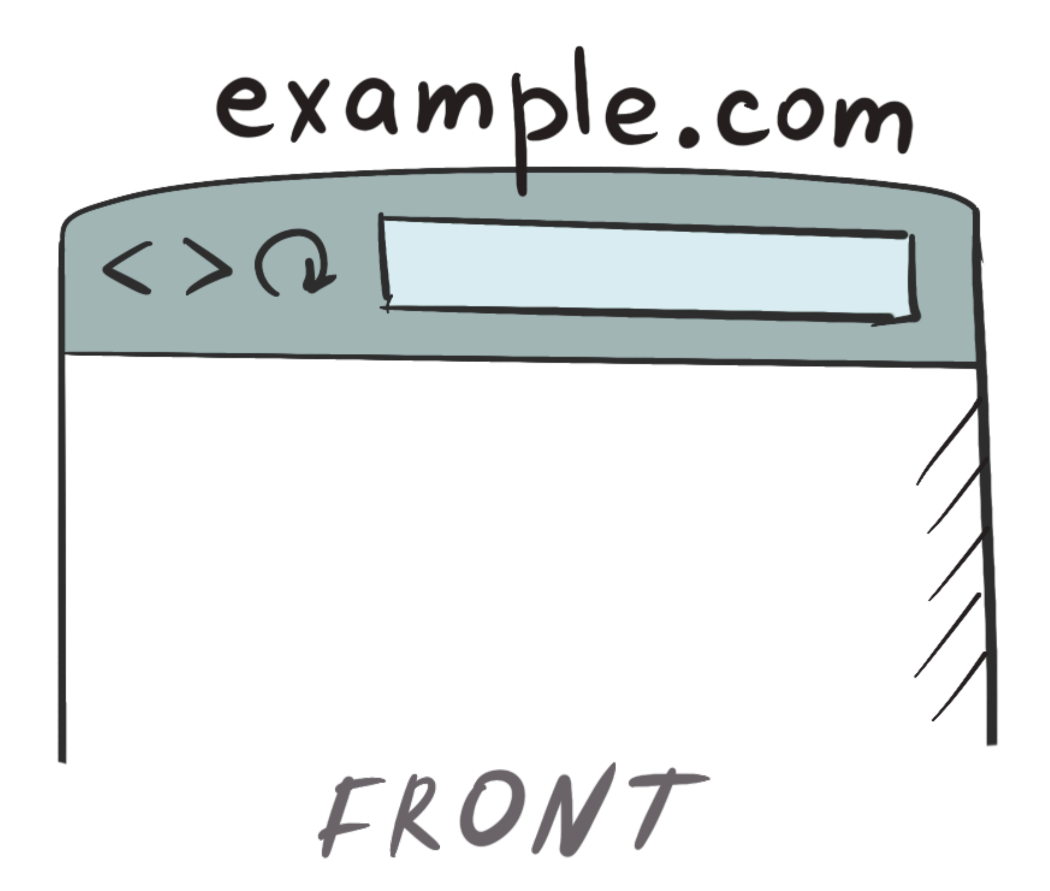


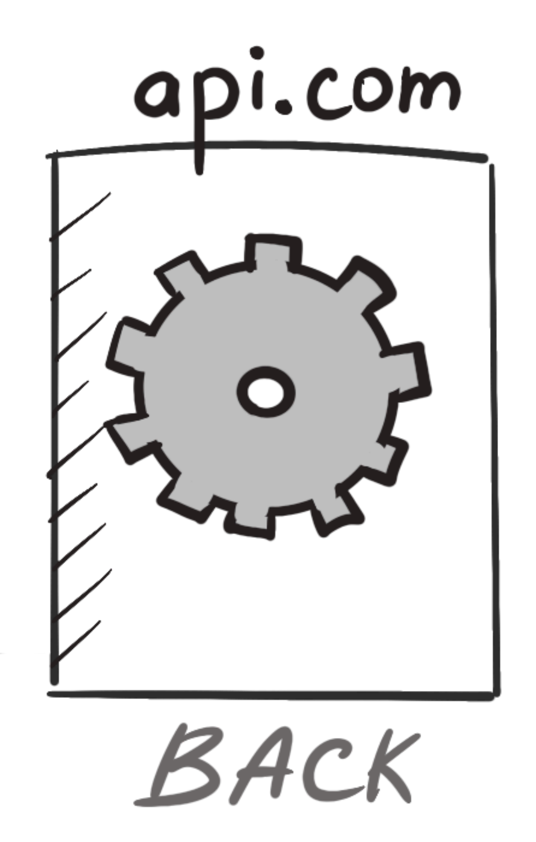
Проблемка

CORS

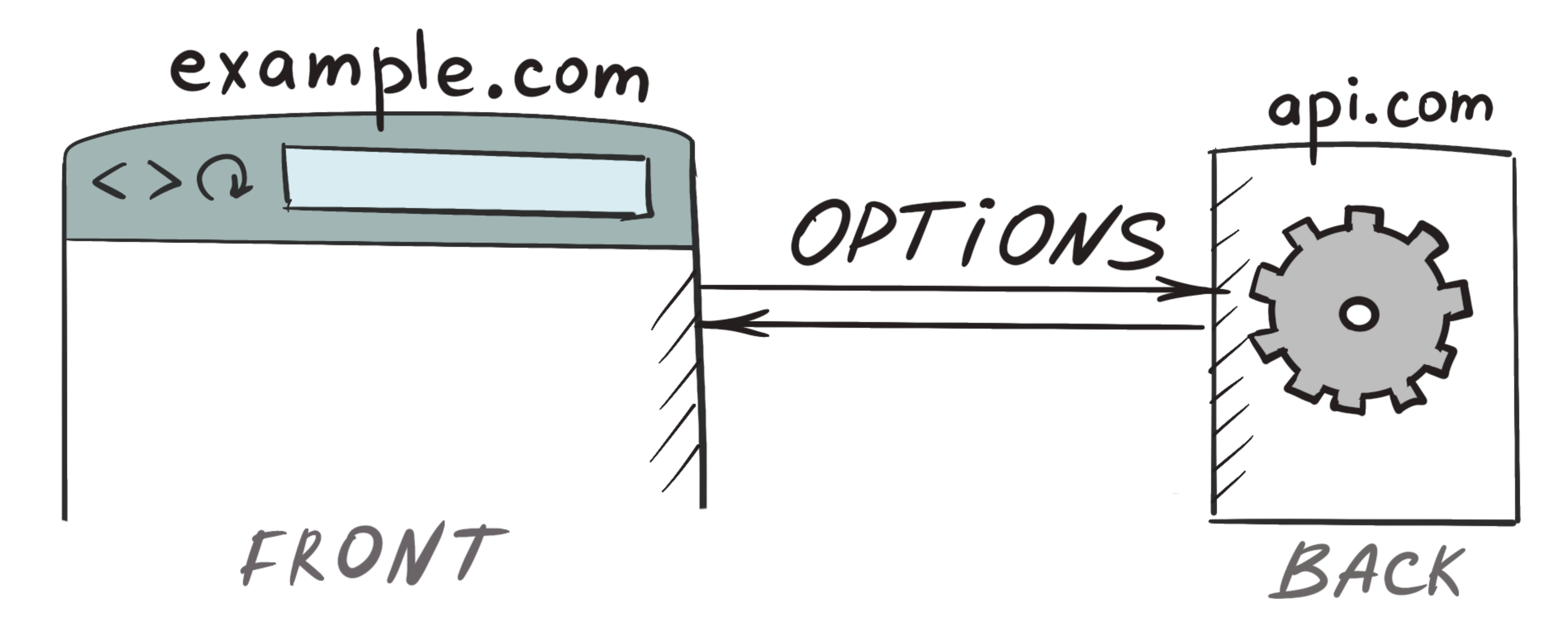
Cross-Origin Resource Sharing

CORS

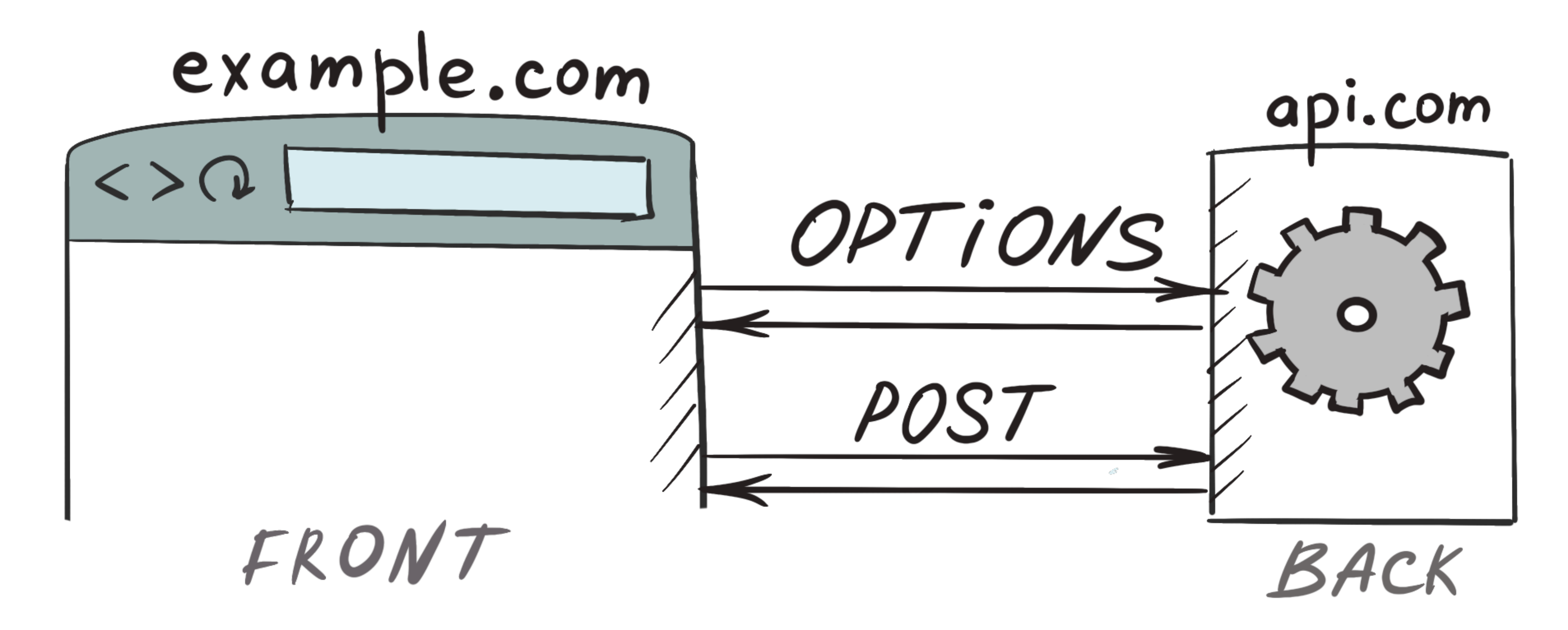




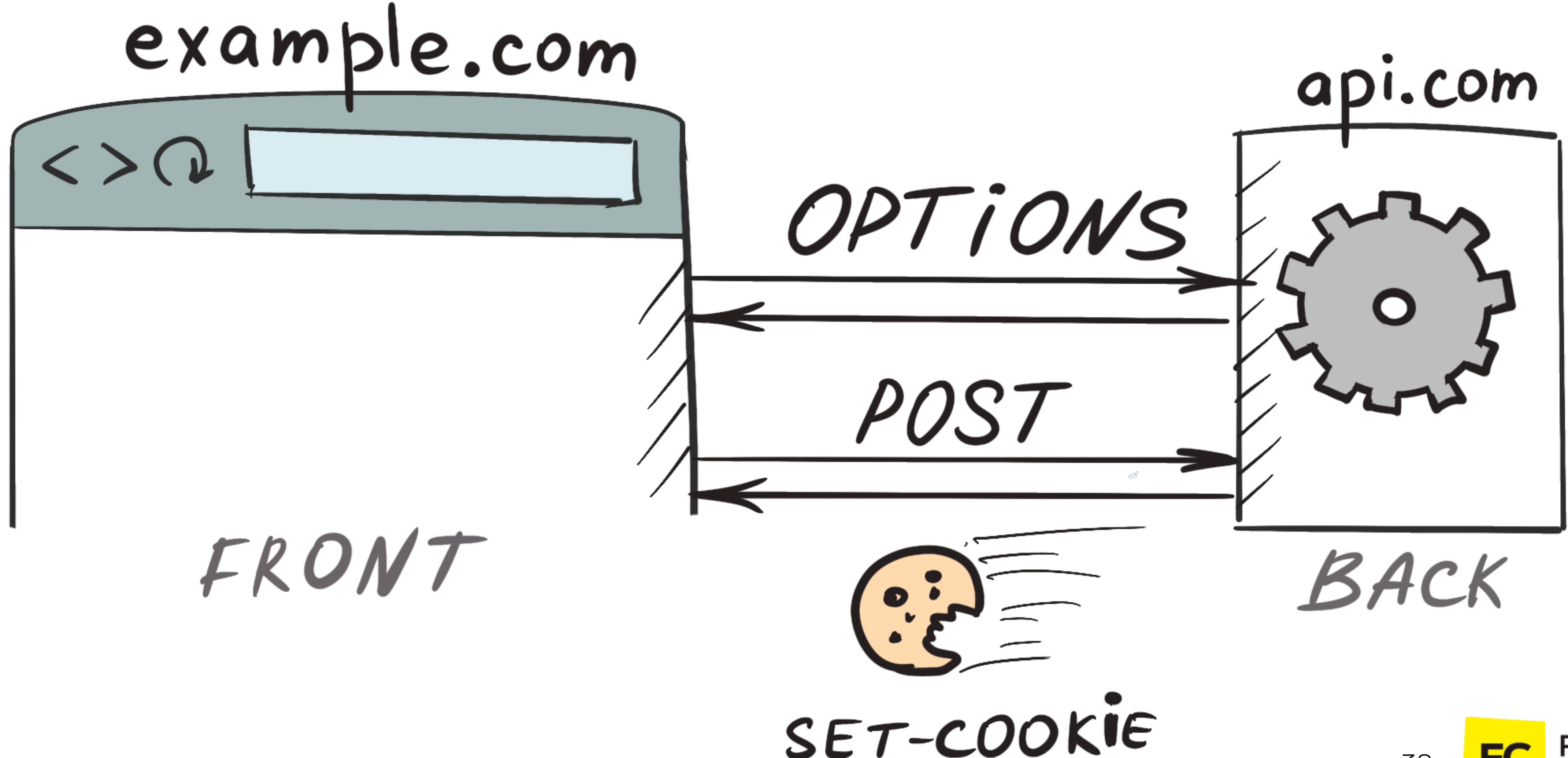
CORS



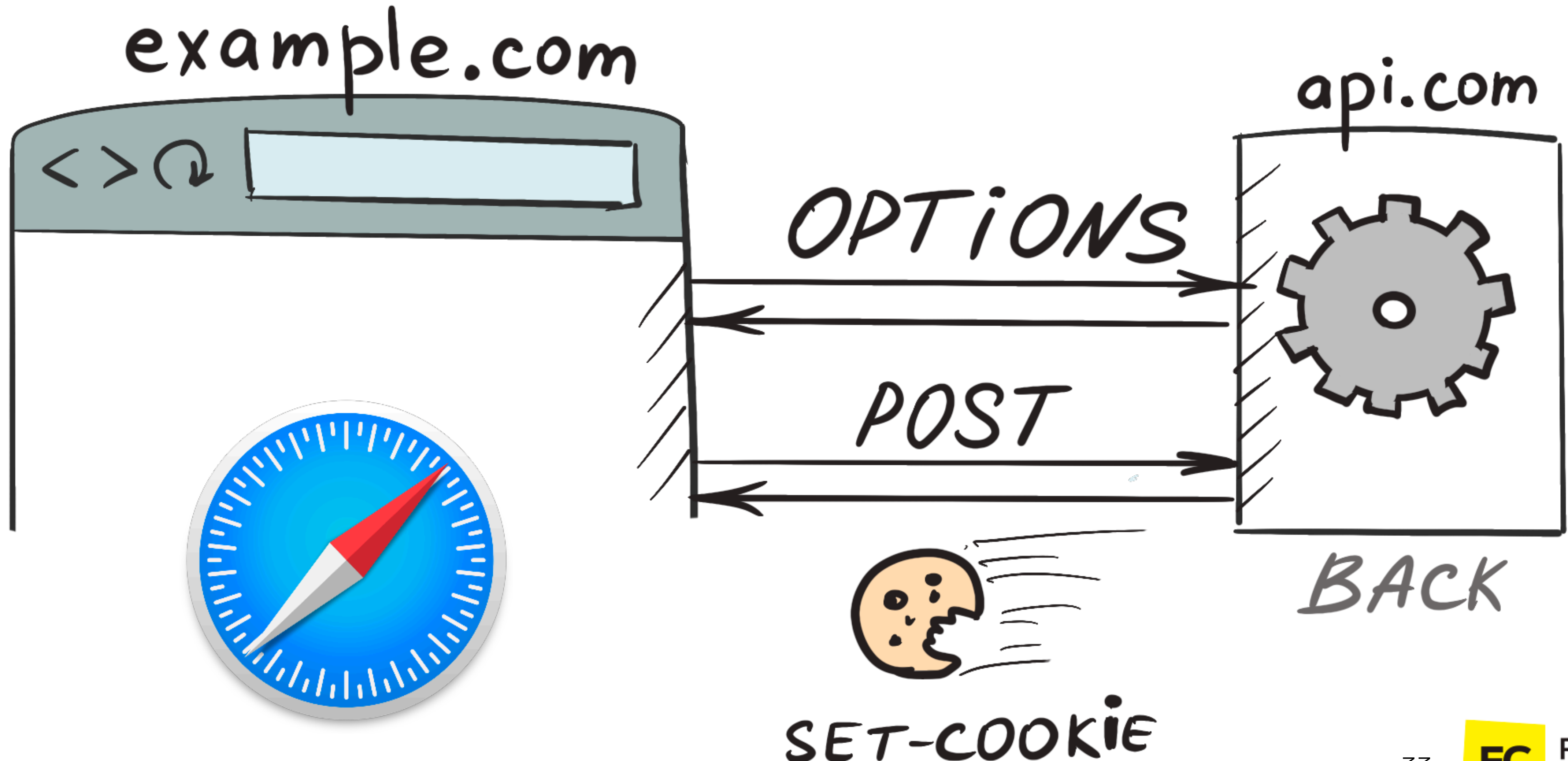
CORS



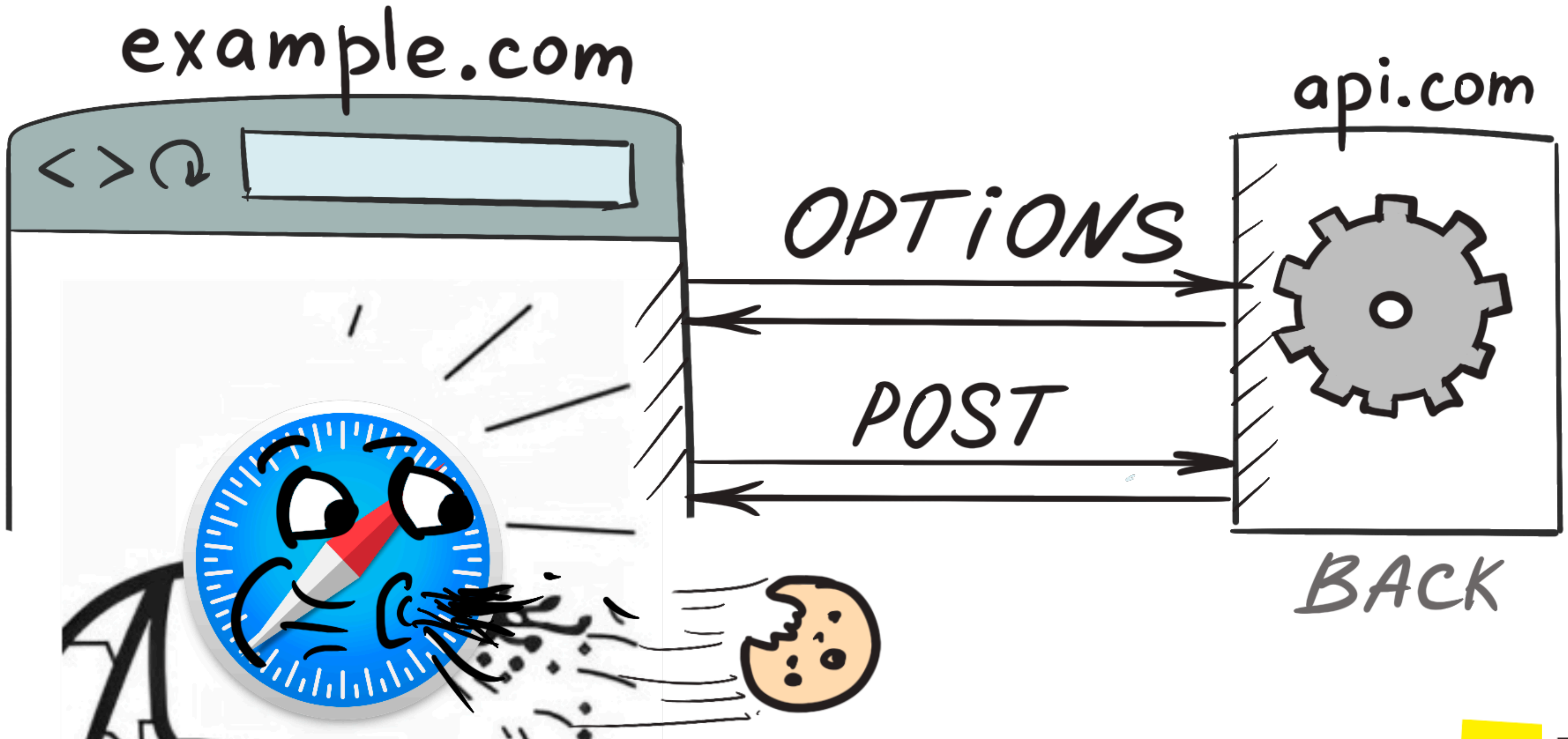
CORS



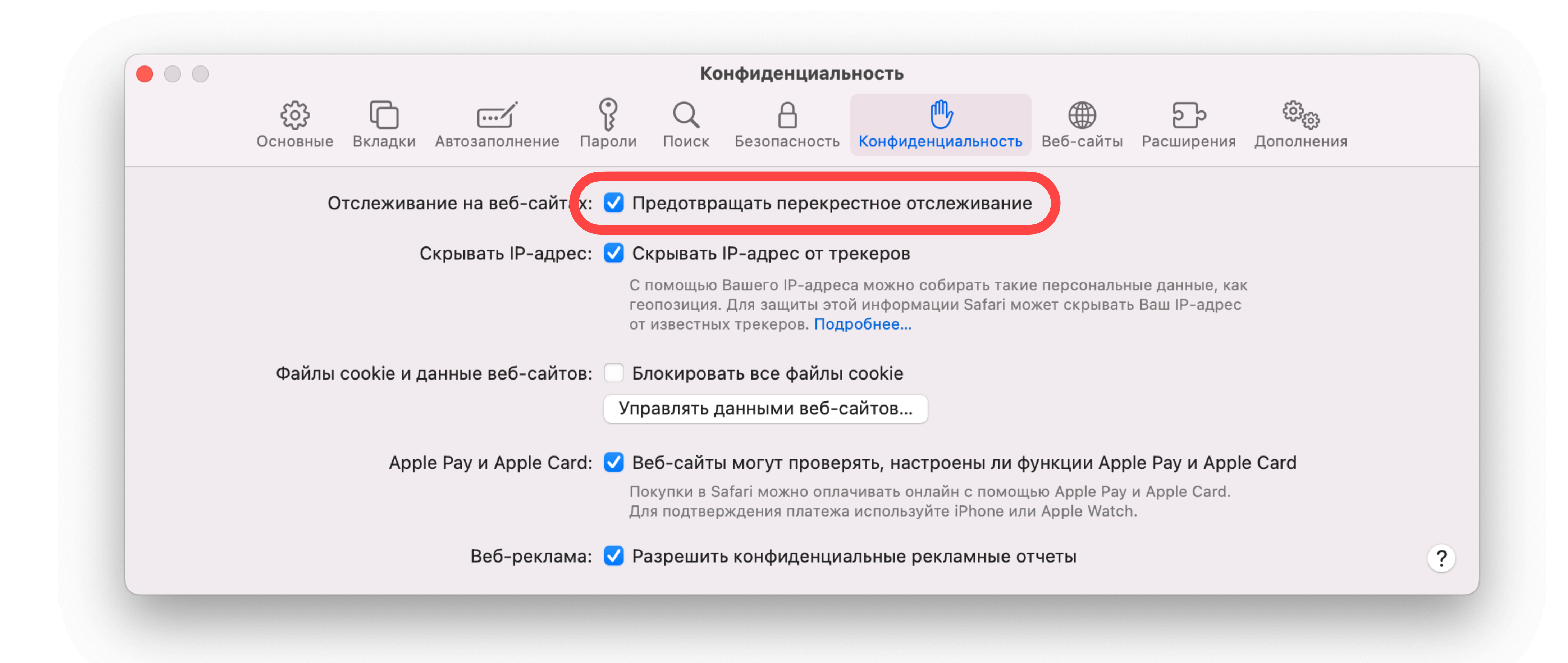
CORS



CORS



Safari против



PCI DSS

Payment Card Industry Data Security Standard (PCI DSS)

Разрешает прием карточных данных на стороне владельца PCI DSS



SHOP.COM

Total 5$

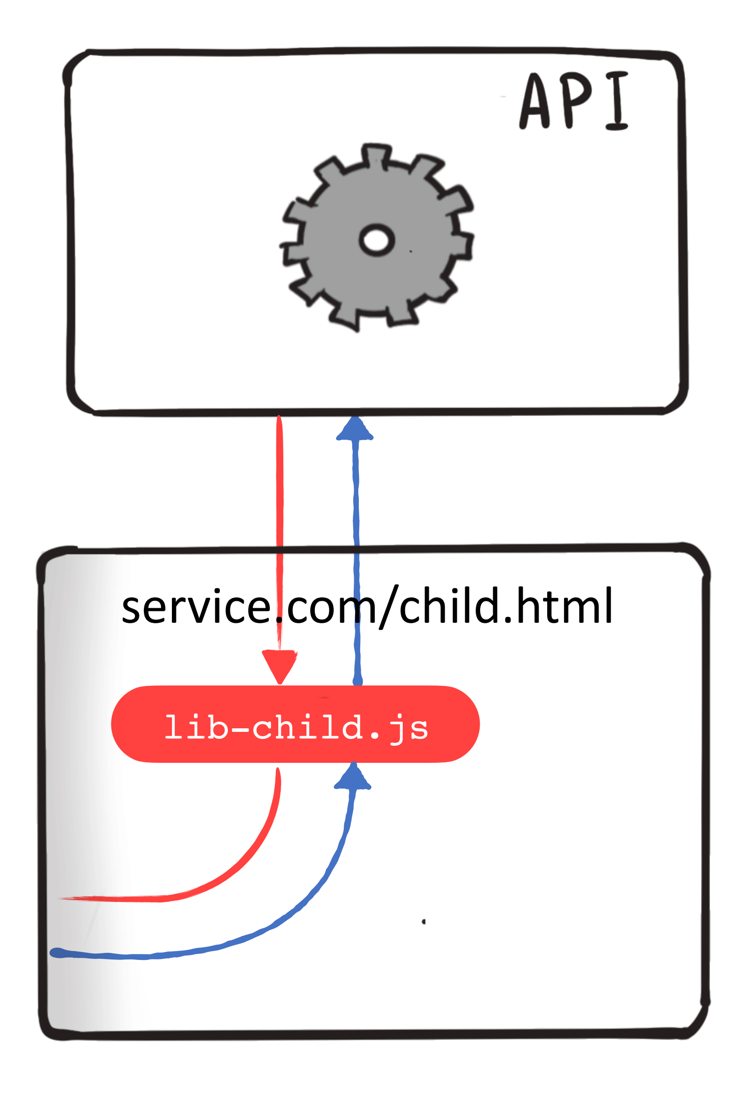
SHOP.COM

Total 5$

Pay

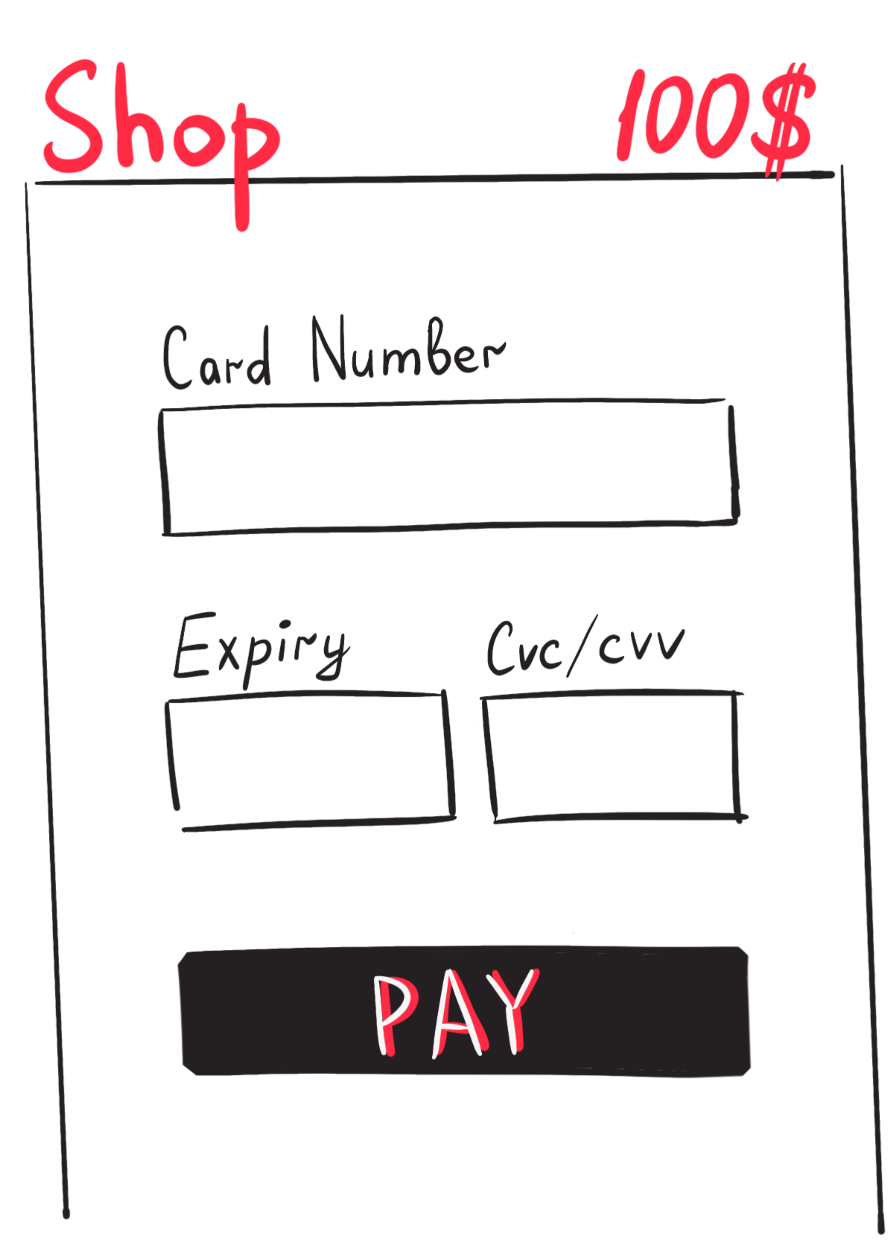
Apple Pay Session

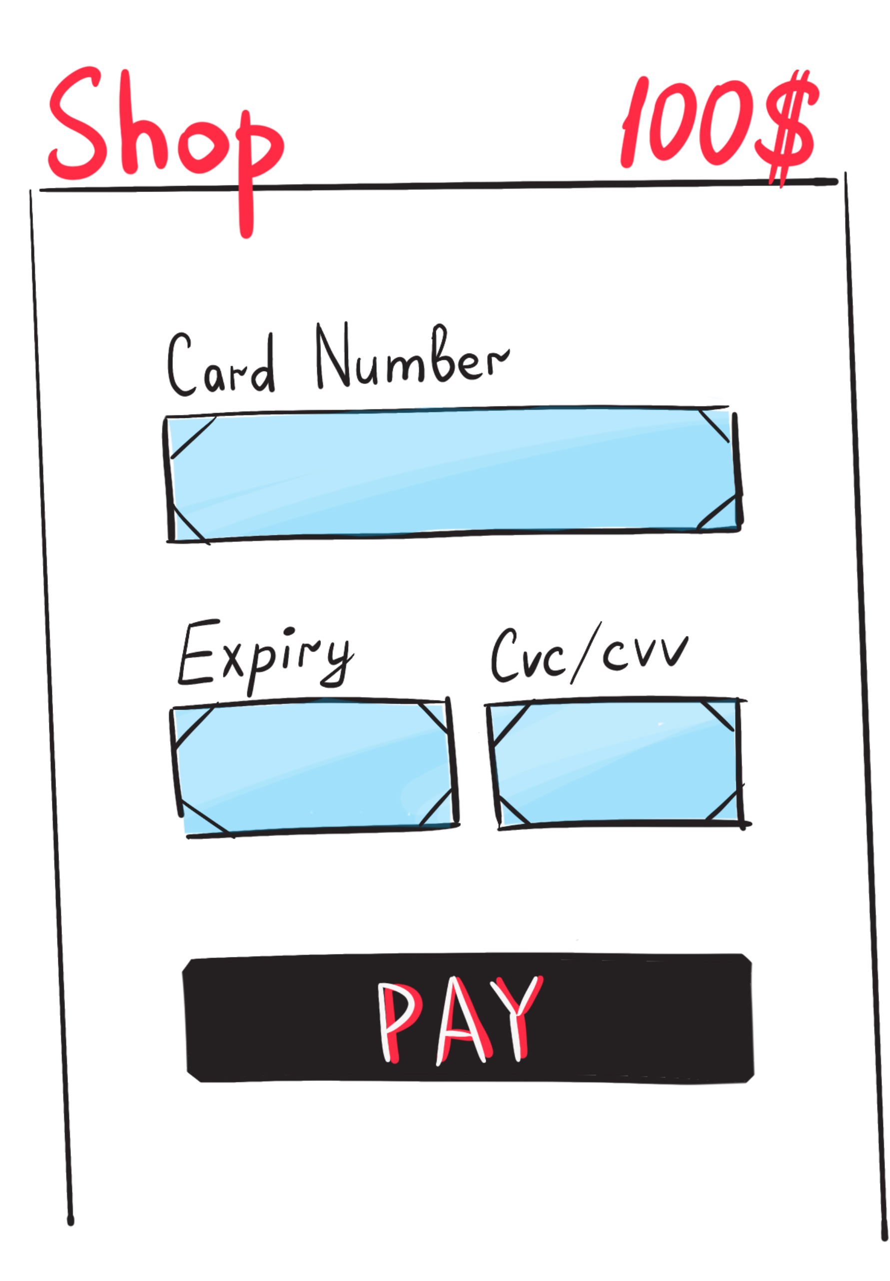
<script src="https://service.com/lib.js">

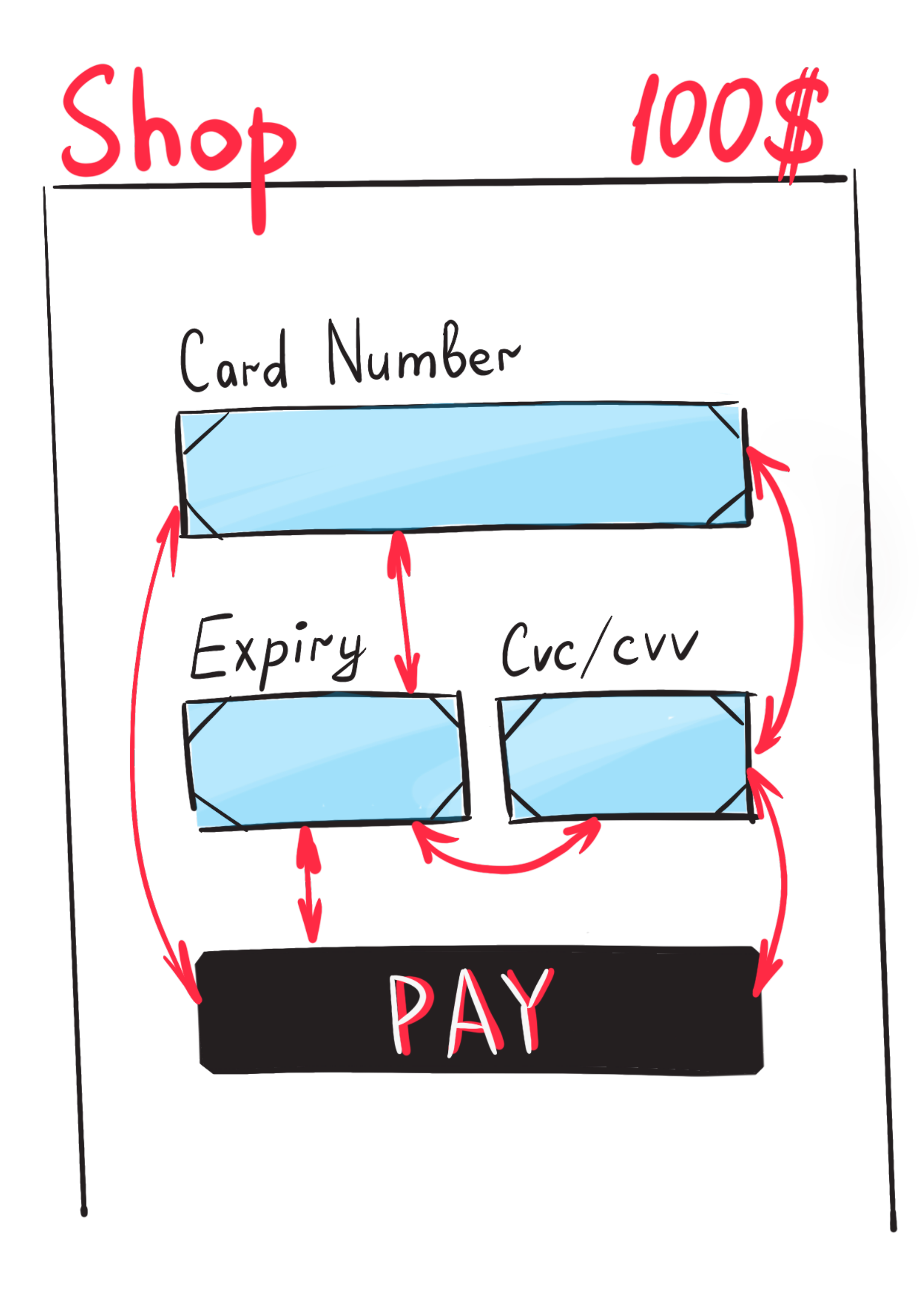


Кроссдоменные запросы через iframe

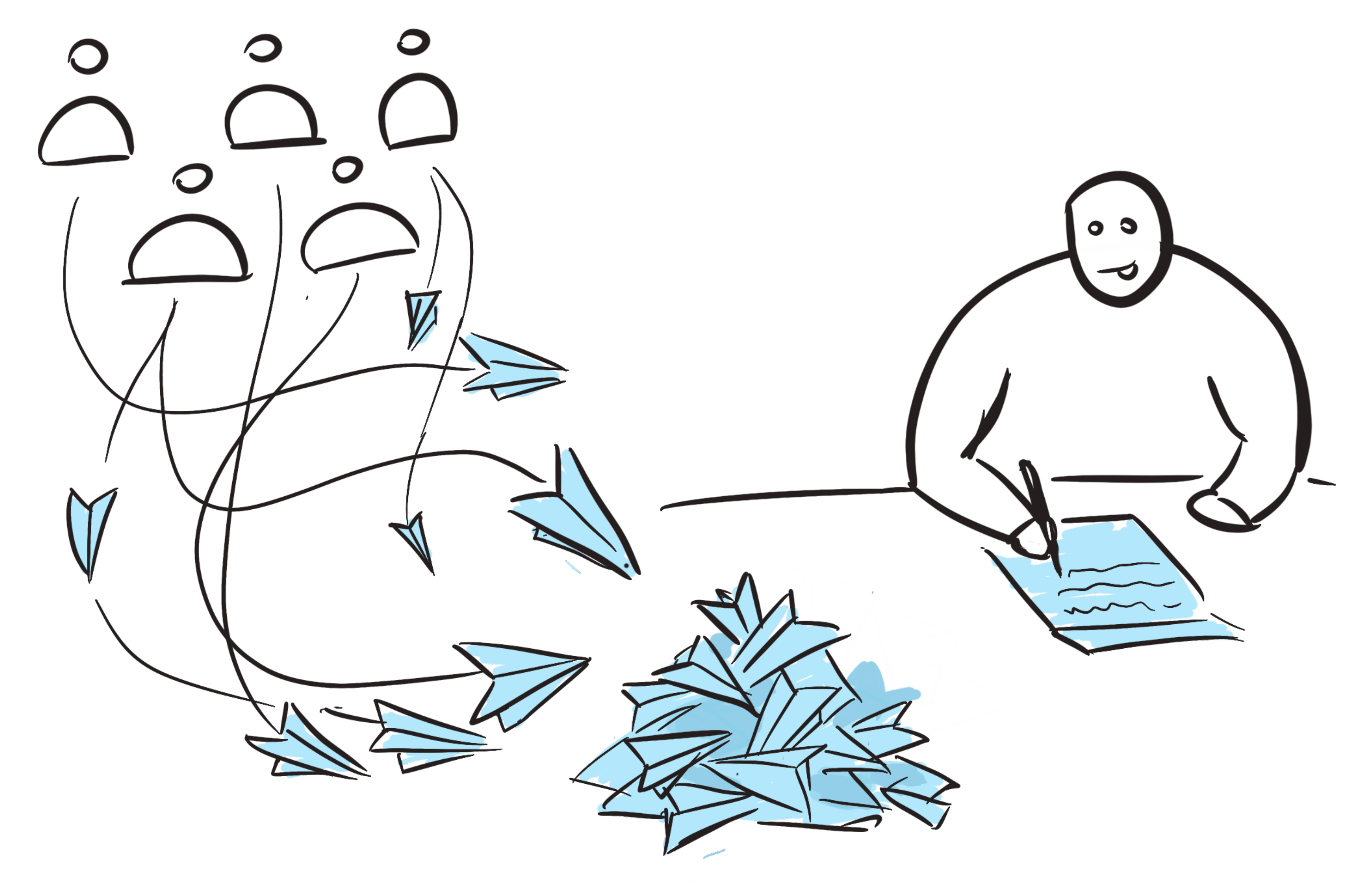
- Не теряет куки
- Владелец сайта не имеет доступа к конфиденциальным данным
- Например, так работает Яндекс.Метрика и Google Analytics

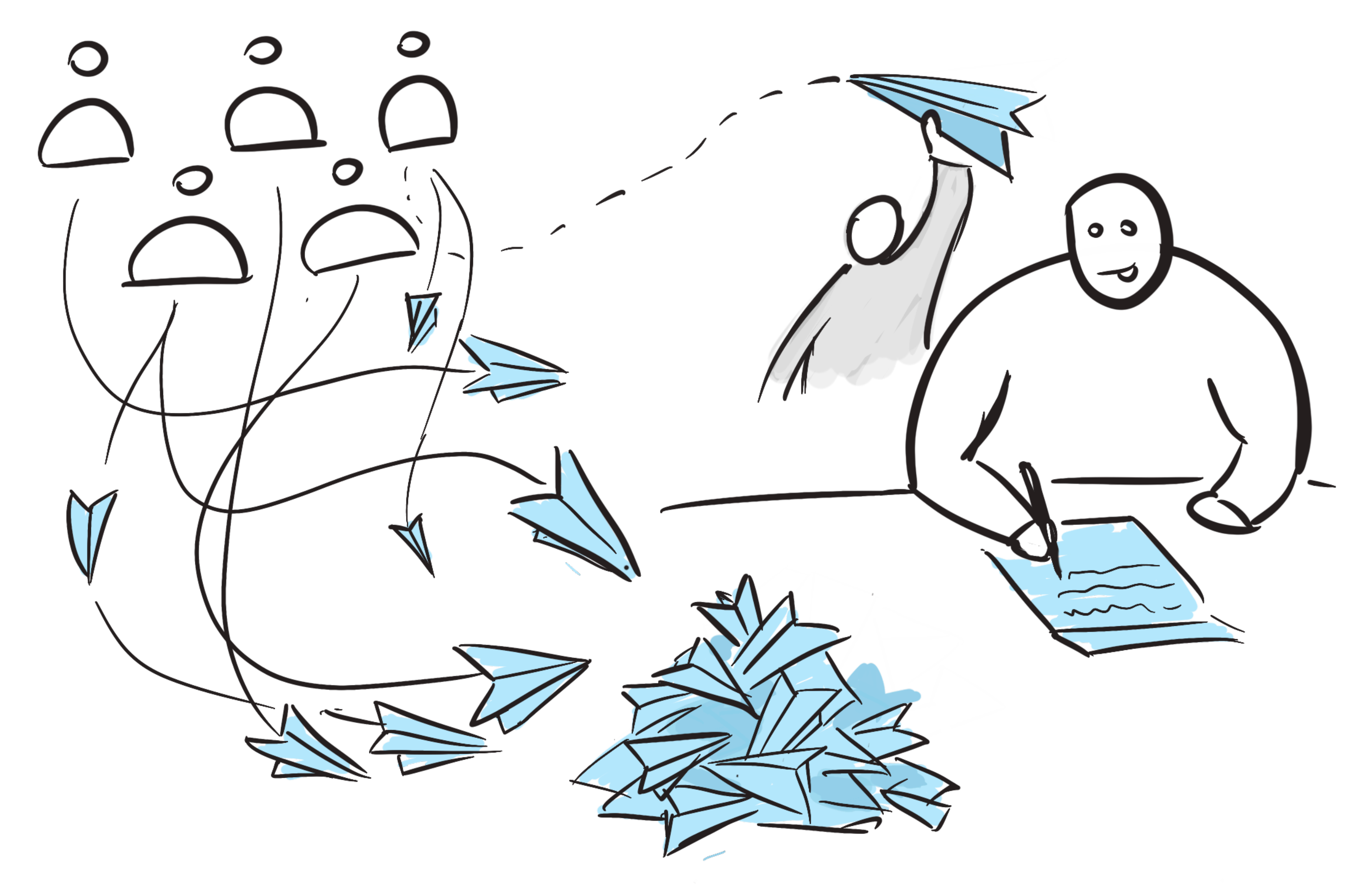

Shop
100$
Card Number
Expiry
Cvc/cvv
PAY

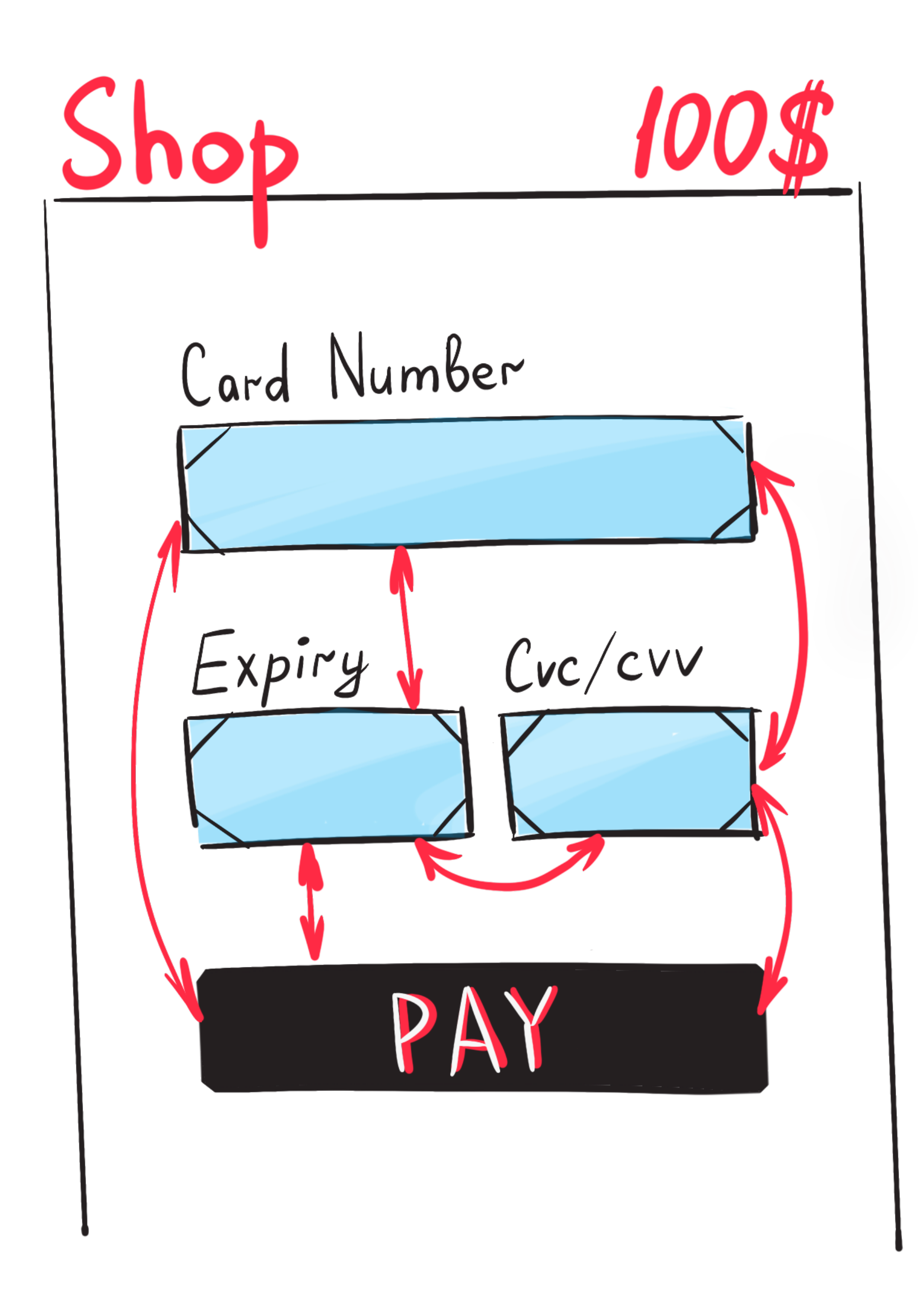

Shop
100$
Card Number
Expiry
Cvc/cvv
PAY

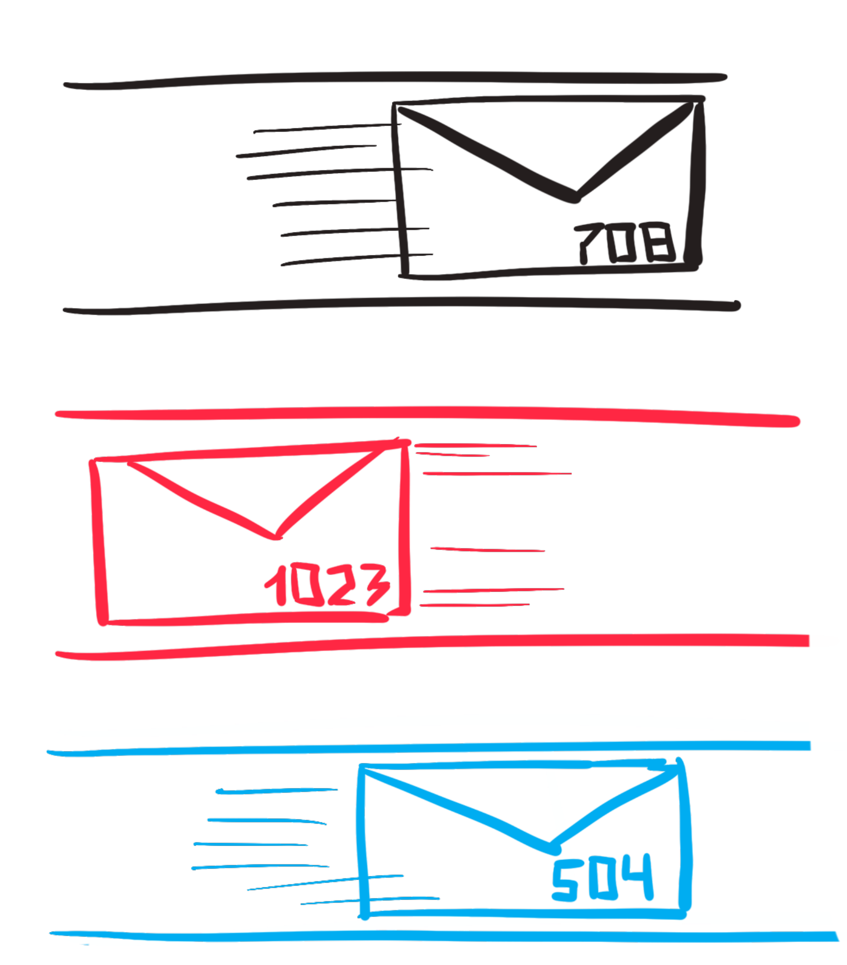

Shop
100$
Card Number
Expiry
Cvc/cvv
PAY








Shop
100$
Card Number
Expiry
Cvc/cvv
PAY


708
1023
504

Shop 100$

Card Number

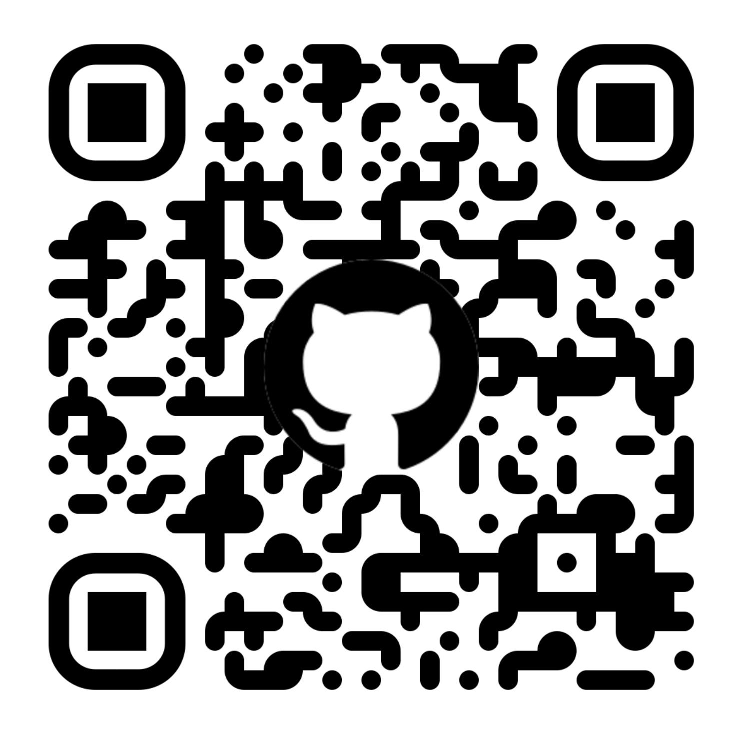
Expiry

Cvc/cvv

PAY

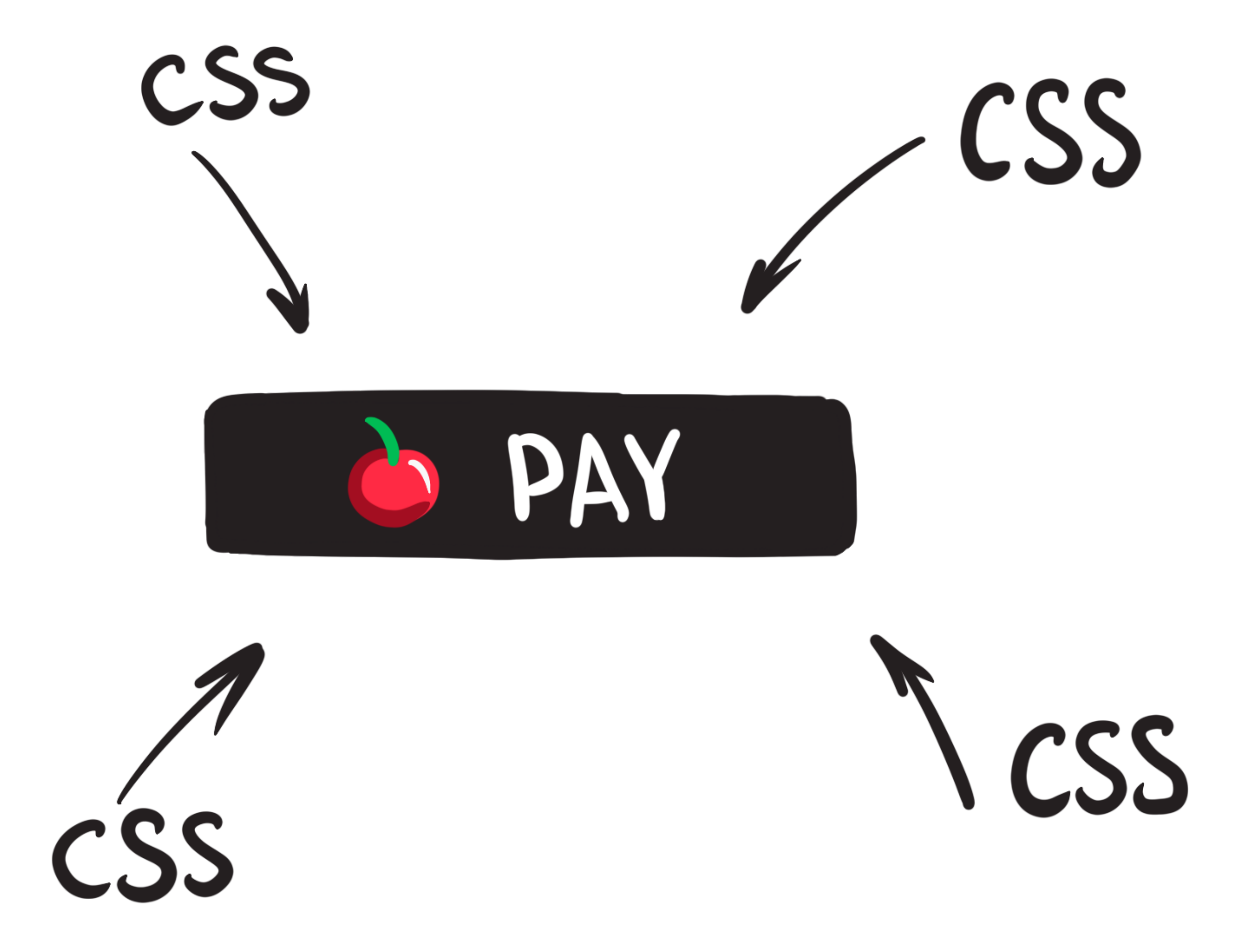
```
type ReqMessageObject = {
  type: 'req';
  funcName: string;
  params: any;
  id: string;
};

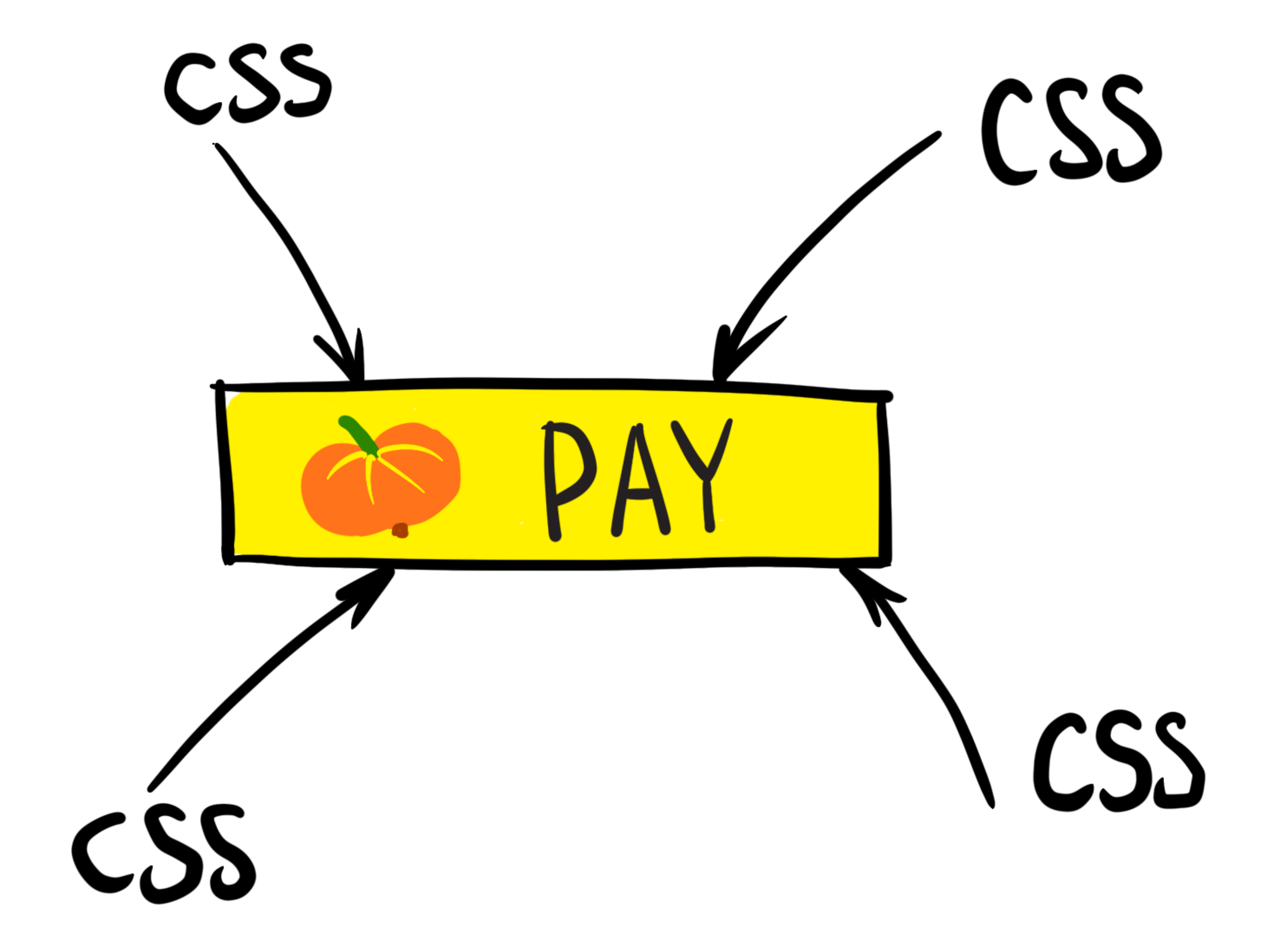
type ResMessageObject = {
  type: 'res';
  result: any;
  error: any;
  id: string;
};
```



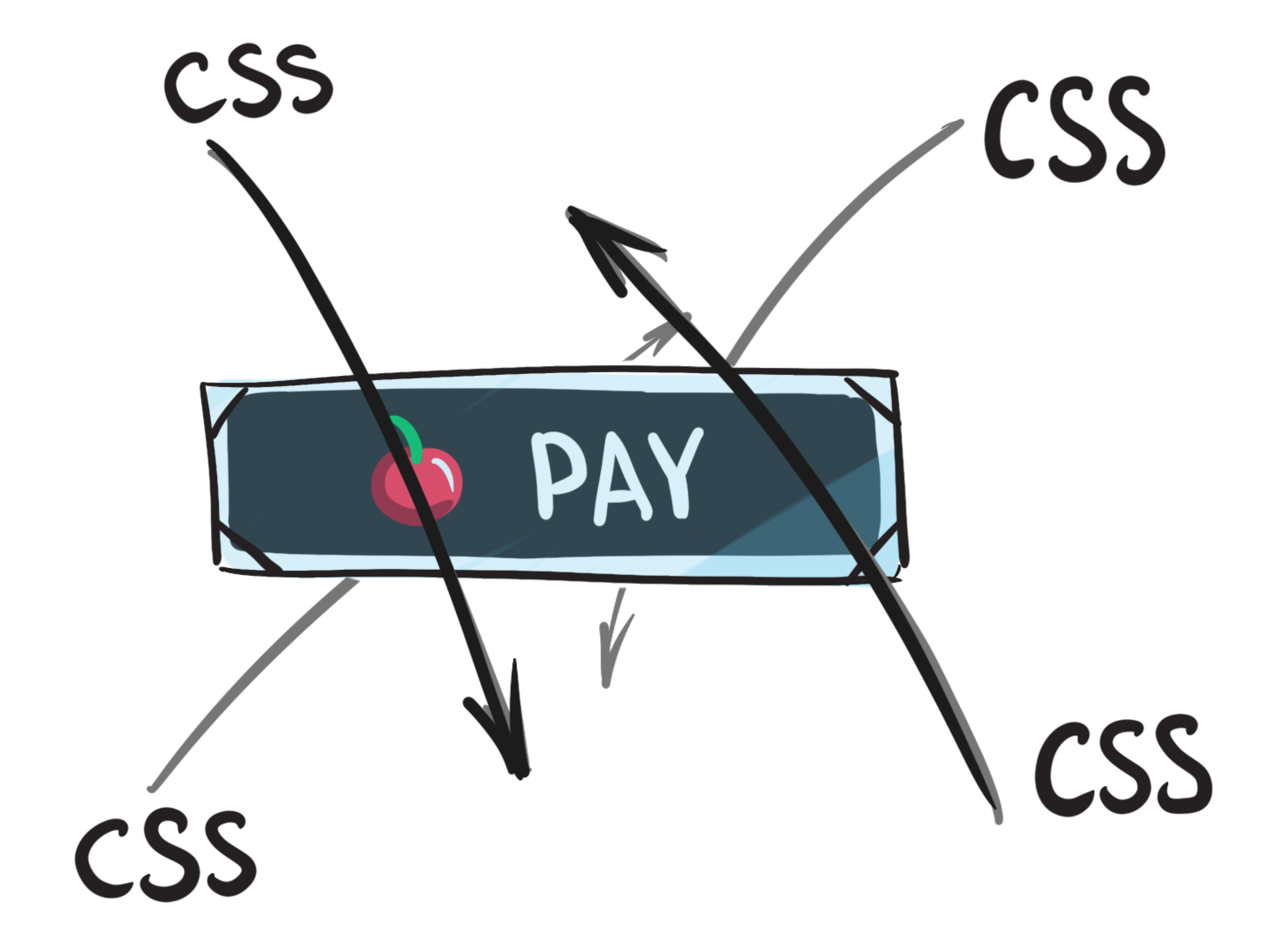
github.com/avin/commutator


PAY


CSS
CSS
PAY
CSS
CSS


CSS
CSS
PAY
CSS
CSS


PAY


CSS
CSS
PAY
CSS
CSS

Порталы

Будущее iframe



Document

portal.liqu.ru

Demo

Lorem ipsum, dolor sit amet consectetur adipisicing elit. Accusamus veritatis qui, quis omnis esse, culpa veniam dignissimos enim voluptates nihil consectetur maxime ipsa, dolores perspiciatis. Ad beatae numquam molestiae non! Voluptatum, odio. Corporis exercitationem ab aut in accusamus dignissimos eaque a fugit dolor quia voluptatem obcaecati assumenda, laborum velit perspiciatis ut blanditiis et nesciunt architecto quos aperiam. Ab error placeat maiores maxime rerum, harum ipsam repudiandae perspiciatis laudantium doloribus

Lorem ipsum dolor sit, amet consectetur adipisicing elit. Voluptatem dicta expedita non ea tempora reprehenderit praesentium autem ex molestiae voluptate, nostrum esse, iste eos veritatis. Magni impedit laudantium animi molestias dolor aspernatur at exercitationem doloribus ratione libero dignissimos, error, minus deleniti iure ullam, nulla sed quam temporibus quo laboriosam quia rem modi fuga. Natus, iure molestiae recusandae suscipit tempore vero magni, eaque voluptas quo sint voluptates totam in? Ipsam maxime inventore repudiandae sapiente minus in aspernatur, dolores labore tempore animi numquam harum odit similique fugiat.
nisi id nostrum facere dolore
non doloremque, perspiciatis asperiores delectus dolorum quisquam
m, optio, totam eum? Totam neque distinctio labore facere
atibus beatae doloremque architecto aliquam possimus incidunt cum,
numquam vitae id quaerat nihil cumque in sunt, nam, ad saepe. Fugit
m sapiente iure explicabo eaque quae maiores ipsum dolore. Enim
m eum sit accusamus quidem repudiandae nobis exercitationem sequi
tas delectus illo hic, incidunt reiciendis minima sed debitis temporibus at
isquam, sapiente voluptates aspernatur ullam dolor. Architecto delectus
ere est culpa quibusdam aspernatur aperiam perferendis voluptatem
mpore vitae accusamus, quo accusantium quod eveniet eos. Similique illo
us ad dignissimos unde ut ratione, quis ducimus eius veritatis
tis quibusdam laudantium dolores velit perferendis. Perferendis
accusamus nulla quaerat sed in optio. Possimus nesciunt quo enim laudantium

FC
Расписание(pdf) Доклады Митапы FAQ Цены Докладчикам Партнёры
купить билет →
личный кабинет
#мыфронтенд
onf FrontendCor
24 и 25 октября 2022 года
Москва, Старт Хаб на Красном Октябре (ex. Digital October)
купить билет
купить видео 2021
стать партнёром



Порталы

FRONT.RU

CONF.RU



Порталы

FRONT.RU

CONF.RU



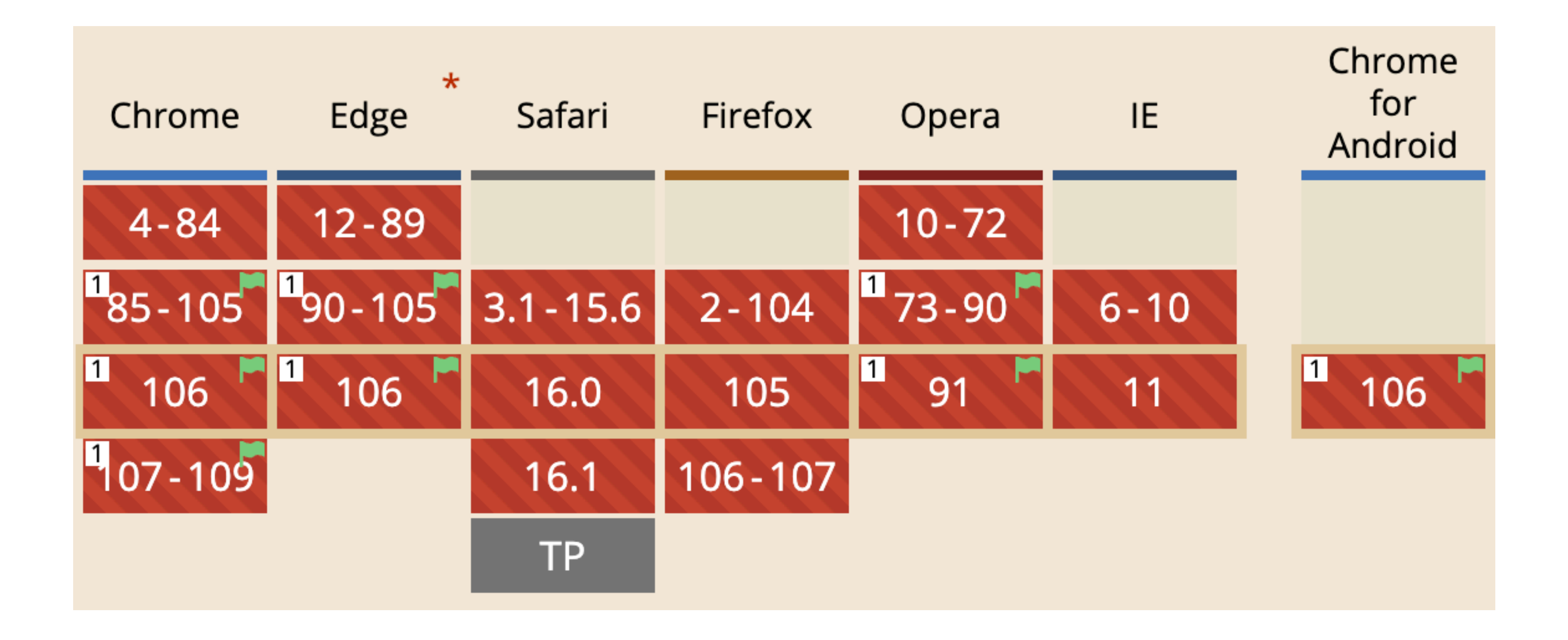
Порталы

```
// Создаем портал со страницей. Как iframe
// Вы можете использовать тег <portal>
portal = document.createElement("portal");
portal.src = "https://frontendconf.ru/moscow/2022";
portal.style = "...";
document.body.appendChild(portal);


// Когда пользователь нажмет на превью портала
// Можно вызвать анимацию, например, увеличение портала
// И закончите, выполнив переход
portal.activate();
```



Порталы



FC Frontend Conf 2022

Порталы

chrome://flags/#enable-portals



- **Enable Portals.**

  Portals are an experimental web platform feature that allows embedding and seamless transitions between pages. See https://github.com/WICG/portals and https://wicg.github.io/portals/ – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

  #enable-portals

  Enabled

- **Enable cross-origin Portals.**

  Allows portals to load cross-origin URLs in addition to same-origin ones. Has no effect if Portals are not enabled. – Mac, Windows, Linux, ChromeOS, Android, Fuchsia, Lacros

  #enable-portals-cross-origin

  Enabled



service.com

SHOP.COM

Total 5$

Pay

Apple Pay Session

redirect

API

RENDER

click

<script src="https://service.com/lib.js">

service.com/child.html

lib-child.js



Заключение

`iframe`

- Развивается, несмотря на возраст.
- Безопасен, если уметь правильно его готовить.
- Временами iframe – единственный вариант для реализации виджетов.

Спасибо за внимание!

Telegram: and_kuznetsov



